

# On the Optimality of Keyless Authentication in a Noisy Model

Shaoquan Jiang

**Abstract**—We further study the keyless authentication problem in a noisy model in our previous work, where no secret setup is available for sender Alice and receiver Bob while there is DMC  $W_1$  from Alice to Bob and a two-way noiseless but insecure channel between them. We propose a construction such that the message length over DMC  $W_1$  does not depend on the size of the source space. If the source space is  $\mathcal{S}$  and the number of channel  $W_1$  uses is  $n$ , then our protocol only has a round complexity of  $\log^* |\mathcal{S}| - \log^* n + 4$ . In addition, we show that the round complexity of any secure protocol in our model is lower bounded by  $\log^* |\mathcal{S}| - \log^* n - 5$ . We also obtain a lower bound on the success probability when the message size on DMC  $W_1$  is given. Finally, we derive the capacity for a non-interactive authentication protocol under general DMCs, which extends the result under BSCs in our previous work.

**Index Terms**—Authentication, information theoretical security, discrete memoryless channel, lower bound, round complexity.

## I. INTRODUCTION

Message authentication is a protocol that allows a sender Alice to send a source state  $S$  to a receiver Bob such that the latter is assured of the authenticity. This mechanism was first studied by [15] in a form of a non-interactive protocol, called a message authentication code (MAC).

Security of an information system usually is quantified through analyzing a number of attacks. There are two types of attacks for a message authentication protocol. In the type I attack, the attacker Oscar plays between Alice and Bob and can modify, block, delete the messages over the channel. He succeeds if Bob finally accepts a source state  $S'$  that is not authenticated by Alice. This is known as a *substitution attack*. In the type II attack, Oscar impersonates Alice to directly authenticate a source state  $S$  to Bob. He succeeds if Bob finally accepts  $S$ . This is known as an *impersonation attack*.

The success probability of Oscar is closely related to his time complexity. A probabilistic polynomial time is a widely adopted complexity class. However, in this work, we are interested in the information theoretical security, where Oscar has an infinite time complexity. The advantage of this type of system is that the security does not rely on any hardness assumption (such as factoring assumption [27]).

To achieve authentication, Alice must have some resource that can distinguish herself from Oscar. For example, if Alice and Bob share a common secret [15], then this secret can play this role. In the literature, a signing key of a signature [27] and a private key [5] of a public key encryption scheme are also examples of this role. In this work, we consider the case,

where a noisy channel for Alice better in some sense than that for Oscar will play as this role.

Channel noise traditionally plays an undesired role in many areas. However, Wyner [30] showed that the channel noise can be used to establish a common secret for Alice and Bob. Csiszár and Körner [12] generalized this result to a broadcast channel. Since then, key agreement over a noisy channel has been extensively studied [1], [14], [19], [2], [23], [24], [6]. Other secure mechanisms over a noisy channel were also studied; see [9], [11], [26] for oblivious transfers and [4], [8], [10], [29] for commitments. Surveys on information theoretical security over noisy channels can be found in [22], [7].

## A. Related works

Authentication that uses a noise as an advantageous resource has been studied in the literature but far from being well-studied (to our knowledge). Baracca et al [3] studied the physical layer authentication over MIMO fading wiretap channels, where they assumed no shared key but an authenticated initialization from the sender to the receiver. Korzhik et al [20] considered an authentication problem over a (noiseless) public discussion channel and an initialization using noisy channels. Lai et al [21] considered a noisy authentication model with a shared key, where the sender-receiver channel is better than the sender-adversary channel. Our previous work [17] studied a new authentication model. In this model, Alice and Bob share no key. There is a discrete memoryless channel  $W_1$  from Alice to Bob and a DMC  $W_2$  from Oscar to Bob. There is also a noiseless channel between any two of Alice, Bob and Oscar. Oscar can read any message from Alice (over channel  $W_1$  or noiselessly) or from Bob (noiselessly) in the clear text. He can also arbitrarily modify the message over the noiseless channel between Alice and Bob. But the message over channel  $W_1$  can not be tampered. In addition, Oscar can impersonate Alice to send any message to Bob using his channel  $W_2$ . A characterization of the (in)existence in this model was given in [17]. Given the existence, an efficient construction was proposed. Further, the non-interactive authentication capacity with BSC  $W_1$  and BSC  $W_2$  was given. Authentication that tries to remove the noise pollution on the data has been studied in the literature. For instance, Martinian et al [25] considered an authentication with a legal distortion and Yu et al [28] considered a covert authentication over a noisy channel. This type of work is not our interest as we consider a noise as an advantageous resource to achieve the authentication.

## B. Contribution

This paper further studies the keyless authentication problem in the noisy model [17]. We extend the construction in [17] to authenticate a source state of any length using a fixed length  $n$  of DMC messages over  $W_1$ , while in [17],  $n$  heavily depends on the size of the source space  $\mathcal{S}$ . Our price is a round complexity of  $\log^* |\mathcal{S}| - \log^* n + 4$  while the protocol in [17] has only 3 rounds. However, we show that the round complexity of any secure protocol in our model must be lower bounded by  $\log^* |\mathcal{S}| - \log^* n - 5$ . This shows that our protocol is nearly round optimal. We remark that this lower bound does not contradict the 3-round protocol in [17] as  $n \geq \frac{\log \log |\mathcal{S}|}{C}$  there, where  $C$  is the Shannon capacity of  $W_1$ . We also obtain a lower bound on the success probability of Oscar. Finally, we obtain the capacity for a non-interactive authentication protocol in our model with general DMCs  $W_1, W_2$  (which extends of the result in [17] with BSC  $W_1$  and BSC  $W_2$ ), where the authentication capacity is the maximum achievable ratio  $\frac{\log |\mathcal{S}|}{n}$ .

## II. PRELIMINARIES

**Notions.** We list notions that will be used later.

- Random variable is abbreviated as RV.
- Denote a RV by a capital letter (e.g.,  $X$ ), its realization by a lower case letter (e.g.,  $x$ ) and its alphabet space by a calligraphic letter (e.g.,  $\mathcal{X}$ ).
- $x^n$  denotes a sequence  $x_1, \dots, x_n$  of length  $n$ .
- $P_X$  is the distribution of  $X$  (i.e.,  $P_X(x) = P(X = x)$ ). Similarly,  $P_{Y|X}(b|a) \stackrel{\text{def}}{=} P(Y = b|X = a)$ .
- $T_{z^n}(\cdot)$  for  $z^n \in \mathcal{Z}^n$  is a distribution over  $\mathcal{Z}$  with  $T_{z^n}(u)$  being the fraction of  $u$  in  $z^n$  for any  $u \in \mathcal{Z}$ .
- $P_X^n(x^n) \stackrel{\text{def}}{=} \prod_{i=1}^n P_X(x_i)$ .
- i.i.d. denotes an independent and identical distribution.
- Function  $\text{negl}(n)$  is *negligible* in  $n$  if for any polynomial  $f(n)$ ,  $\lim_{n \rightarrow \infty} \text{negl}(n)f(n) = 0$ .
- $\log^{(j)} x = \underbrace{\log \cdots \log}_j(x)$  (i.e., the composition of  $\log$  function for  $j$  times).
- $\log^* n$  is the minimum  $i$  such that  $\log^{(i)} n < 2$ .
- Convex hull  $\text{Cov}(S)$  for a set  $S$  of vectors is the set of all possible convex combinations of vectors in  $S$ .
- $[n]$  denote the set  $\{1, \dots, n\}$ .
- For  $S \subseteq [p]$  and a matrix  $W = (W_1, \dots, W_p)^T$  with row vectors  $W_1, \dots, W_p$ , define  $W_S = \{W_s \mid s \in S\}$ .
- Statistical distance between RVs  $X$  and  $X'$  is  $\Delta(X, X') = \sum_x |P_X(x) - P_{X'}(x)|$ . We also denote it by  $\Delta(P_X, P_{X'})$ . For any distribution  $P$  over  $\mathcal{X}$  and a *compact* set of distributions  $\mathcal{S}$  over  $\mathcal{X}$ , define  $\Delta(P, \mathcal{S}) = \min_{Q \in \mathcal{S}} \Delta(P, Q)$ .
- Hamming distance  $d_H(x^n, y^n) = |\{i \mid x_i \neq y_i, i \in [n]\}|$ .
- The binary entropy function  $h(\alpha) = -\alpha \log \alpha - (1 - \alpha) \log(1 - \alpha)$  for  $\alpha \in [0, 1]$ .

### A. Discrete memoryless channel

A discrete channel with input  $X$  over  $\mathcal{X} = \{a_1, \dots, a_p\}$  and output  $Y$  over  $\mathcal{Y} = \{b_1, \dots, b_q\}$  is denoted by a stochastic

matrix

$$W = \begin{pmatrix} W(b_1|a_1) & \cdots & W(b_q|a_1) \\ \vdots & \ddots & \vdots \\ W(b_1|a_p) & \cdots & W(b_q|a_p) \end{pmatrix},$$

where  $W(y|x) = P_{Y|X}(y|x)$ . In this case, we say  $X$  and  $Y$  are *connected by channel*  $W$ . The channel is *discrete memoryless* (DMC) if  $P_{Y^n|X^n}(y^n|x^n) = \prod_{i=1}^n W(y_i|x_i)$ . It is *non-redundant* if  $\Delta(W_i, \text{Cov}(W_{[p] \setminus \{i\}})) > 0$  for any  $i \in [p]$ .

A  $n$ -length code  $\mathcal{C}$  for  $W : \mathcal{X} \rightarrow \mathcal{Y}$  with source  $\mathcal{S}$  is described by an encoding scheme  $f : \mathcal{S} \rightarrow \mathcal{X}^n$  and a decoding scheme  $\phi : \mathcal{Y}^n \rightarrow \mathcal{S} \cup \{\perp\}$ . A decoding result  $\perp$  denotes a detection of error. For  $S \in \mathcal{S}$ ,  $f(S) \in \mathcal{X}^n$  is called a *codeword*. When  $f(S)$  is sent over  $W$  and received as  $Y^n \in \mathcal{Y}^n$ , the receiver will decode it to  $\phi(Y^n)$ . If  $\phi(Y^n) \neq S$ , an error occurs. The *error probability* is  $P(\phi(Y^n) \neq S)$ .

### B. Typical sequences

In this subsection, we introduce the notions of typical and conditional typical sequences [13].

**Definition 1:** Let  $X$  be a RV over  $\mathcal{X}$ . We say that  $x^n \in \mathcal{X}^n$  is  $\epsilon$ -*typical* if  $|T_{x^n}(a) - P_X(a)| \leq \frac{\epsilon}{|\mathcal{X}|}$  for any  $a \in \mathcal{X}$  and whenever  $P_X(a) = 0$ , it holds that  $T_{x^n}(a) = 0$ . The set of  $\epsilon$ -typical sequences for  $X$  is denoted by  $\mathcal{T}_{[X]_\epsilon}^n$ .

**Definition 2:** Let  $X$  and  $Y$  be RVs over  $\mathcal{X}$  and  $\mathcal{Y}$  respectively.  $y^n \in \mathcal{Y}^n$  is *conditionally  $\epsilon$ -typical* given  $x^n \in \mathcal{X}^n$ , if  $|T_{x^n y^n}(a, b) - T_{x^n}(a)P_{Y|X}(b|a)| \leq \frac{\epsilon}{|\mathcal{X}| \cdot |\mathcal{Y}|}$  for all  $a \in \mathcal{X}, b \in \mathcal{Y}$  and whenever  $P_{XY}(a, b) = 0$ , it holds that  $T_{x^n y^n}(a, b) = 0$ . The set of conditionally  $\epsilon$ -typical sequences for  $Y$ , given  $x^n$ , is denoted by  $\mathcal{T}_{[Y|X]_\epsilon}^n(x^n)$ , and also by  $\mathcal{T}_{[W]_\epsilon}^n(x^n)$  if  $X$  and  $Y$  are connected by DMC  $W$ .

The following is a basic property of typical sequences. The proof can be found in [13, Chapter 2].

**Lemma 1:** Let  $X$  and  $Y$  be RVs over  $\mathcal{X}$  and  $\mathcal{Y}$  respectively. Then, there exists constants  $\lambda_1 > 0$  and  $\lambda_2 > 0$  such that

$$P_Y^n(\mathcal{T}_{[Y]_\epsilon}^n) \geq 1 - 2^{-n\lambda_1\epsilon^2}$$

$$P_{Y|X}^n(\mathcal{T}_{[Y|X]_\epsilon}^n(x^n)|x^n) \geq 1 - 2^{-n\lambda_2\epsilon^2}, \quad \forall x^n \in \mathcal{T}_{[X]_\epsilon}^n,$$

when  $n$  large enough.

### C. Basic inequalities

The following lemma is from [17]. It essentially states that if the distribution  $T_{Z^n}$  induced by the output  $Z^n$  of a DMC  $W$  is close to a distribution  $P$ , then  $P$  must be close to  $\text{Cov}(W)$ .

**Lemma 2:** Let  $P$  be a distribution over  $\mathcal{Z}$ . Let  $Z^n$  be an output of DMC  $W : \mathcal{X} \rightarrow \mathcal{Z}$  with input  $X^n$ . If

$$P_{Z^n} \left( |T_{Z^n}(u) - P(u)| \leq \epsilon_1, \text{ for all } u \in \mathcal{Z} \right) > \epsilon_2, \quad (1)$$

for some  $\epsilon_1, \epsilon_2 > 0$ , then

$$\Delta(P; \text{Cov}(W)) \leq |\mathcal{Z}|\epsilon_1 + |\mathcal{Z}|\sqrt{\frac{\ln(2/\epsilon_2)}{2n}}. \quad (2)$$

The next lemma is taken from [18]. It essentially states that if  $x^n$  and  $\bar{x}^n$  has a large distance, then sending  $x^n$  through a

non-redundant DMC  $W$  is unlikely to result in an output  $Y^n$  that is conditionally  $\epsilon$ -typical with  $\bar{x}^n$ .

**Lemma 3:** Let  $Y^n$  be the output of a non-redundant DMC  $W : \mathcal{X} \rightarrow \mathcal{Y}$  with input  $X^n$ . Then for any  $x^n, \bar{x}^n \in \mathcal{X}^n$  with  $d_H(\bar{x}^n, x^n) = \alpha n$ , any  $\epsilon \in (0, \Theta\alpha)$  and  $\alpha > 0$ , it holds that

$$P_{Y^n|X^n} \left( T_{[W]_\epsilon}^n(\bar{x}^n) | x^n \right) \leq 2^{-\frac{2n(\alpha\Theta - \epsilon)^2}{|\mathcal{X}|^2|\mathcal{Y}|^2}}, \quad (3)$$

where  $\Theta = \min_i \Delta \left( W_i, \text{Cov}(W_{[p] \setminus \{i\}}) \right)$  and the rows of  $W$  are  $W_1, \dots, W_p$ .

The following lemma is a special case of [18, Lemma 6].

**Lemma 4:** For  $1/n \leq \alpha \leq 1/2$ , there exists a subset  $V_\alpha \subseteq \mathcal{X}^n$  with

$$|V_\alpha| \geq \frac{1}{\alpha n} |\mathcal{X}|^n 2^{-n(h(\alpha) + \alpha \log |\mathcal{X}|)}$$

such that  $d_H(x_1^n, x_2^n) \geq \alpha n$  for any distinct  $x_1^n, x_2^n \in V_\alpha$ .

#### D. $(v, b, r, \lambda)$ -Set System

We now introduce the  $(v, b, r, \lambda)$ -set system in [17], which is extended from block design [16].

**Definition 3:** Let  $V$  be a set of size  $v$  and  $\mathcal{B} = \{\mathcal{B}_1, \dots, \mathcal{B}_b\}$  (called *blocks*) be a collection of subsets of  $V$ . Then,  $(V, \mathcal{B})$  is a  $(v, b, r, \lambda)$ -set system if

1. Each  $x \in V$  belongs to at least  $r$  blocks.
2. Any  $x, y \in V$  simultaneously appear in at most  $\lambda$  blocks.

The following lemma is a rephrase of an existence result proved in [17].

**Lemma 5:** Let  $v, b, t \in \mathbb{N}$  with  $b = \lfloor \frac{2^{t+s}}{\epsilon^4} \log v \rfloor$  and  $v \geq 2$  and  $0 < \epsilon < 1$ . Then, there exists a  $(v, b, 2^{-25t-2}\epsilon b, 2^{-5t-2}\epsilon^2 b)$ -set system.

The above lemma shows that the existence of a set system with  $b > 512\epsilon^{-4} \log v$ . We now prove that  $b > \log v$  actually holds for any set system with  $\epsilon < 1$ . Although this result will not be directly used in this paper, it is the main motivation that leads us to the lower bound on the round complexity in Section V.

**Lemma 6:** Let  $(V, \mathcal{B}_1, \dots, \mathcal{B}_b)$  be a  $(v, b, r, \lambda)$ -set system with  $\lambda < r$ . Then,  $b > \log v$ .

**Proof.** For any  $s \in V$ , define a  $b$ -bit string  $I(s)$ , where the  $i$ th bit  $I(s)_i = 1$  if and only if  $s \in \mathcal{B}_i$ . As any distinct  $s_1, s_2 \in V$  simultaneously appear in at most  $\lambda < r$  blocks while each of  $s_1, s_2$  appears in at least  $r$  blocks, it follows that  $I(s_1) \neq I(s_2)$ . Hence,  $I(\cdot)$  is an injection from  $V$  to  $\{0, 1\}^b$ . Since  $I(s)$  is a  $b$ -bit string with at least  $r$  positions being 1,  $v \leq 2^b - \sum_{i=0}^{r-1} \binom{b}{i}$ . That is,  $b > \log v$ .  $\square$

### III. AUTHENTICATION MODEL

In this section, we introduce the noisy authentication model over DMCs in [17]. It consists of two DMCs:  $W_1 : \mathcal{X} \rightarrow \mathcal{Z}$  from Alice to Bob and DMC  $W_2 : \mathcal{Y} \rightarrow \mathcal{Z}$  from Oscar to Bob. Between Alice and Bob, there exists a two-way noiseless channel. Alice will use  $W_1$  and the noiseless channel to authenticate a source state to Bob. Oscar is an attacker. He can read the messages sent over the two-way noiseless channel and channel  $W_1$ . He can also tamper the messages on the two-way noiseless channel. Allowing Oscar to control the noiseless channel is to capture the concern that this channel is neither

confidential nor authenticated. Allowing Oscar to see Alice's message over the DMC  $W_1$  is to capture the concern that this channel may leak some information. One might think that let Oscar know the full input of  $W_1$  is unnecessary. However, we prefer this as it simplifies the model and also provides a stronger security guarantee.

After rounds of interactions, Bob can decide whether to accept the authentication. When he accepts, he outputs a source state; otherwise, he outputs a special symbol  $\perp$ . If Bob detects an error before completing the interaction, he outputs  $\perp$  and aborts immediately. The formal description follows.

1) *Communication model:* Let  $\mathcal{S}$  be the source space, from which Alice draws a source state  $S$  for authentication. Let  $\pi_n$  be a  $\nu$ -round authentication protocol with totally  $n$  symbols transmitted over channel  $W_1$ . Each party has a basic input and a random input (a uniformly random binary string which is the randomness source in the execution for this party). Alice's basic input is  $S$  and random input is  $r_A$ , while Bob's basic input is empty and random input is  $r_B$ . If the list of messages a party has received so far is  $T$ , then his (or her) next action (e.g., generating a local output, an outgoing message or making a reject/accept decision) is completely determined by his basic input, random input and  $T$ . We use  $\pi_n(A, r_A, T)$  to denote Alice's next action function and  $\pi_n(B, r_B, T)$  to denote Bob's next action function. The interaction is as follows, where  $n = \sum_{i=1}^\nu n_i$ .

A-1: Alice computes  $(X_1^{n_1}, u_1) = \pi_n(A, S, r_A)$ . She sends  $X_1^{n_1}$  over channel  $W_1$  and  $u_1$  over the noiseless channel, to Bob. Oscar will see  $X_1^{n_1}, Z_1^{n_1}$  and  $u_1$ . He can modify  $u_1$  to  $u'_1$ . Bob will receive  $Z_1^{n_1}$  from channel  $W_1$  and  $u'_1$  from the noiseless channel.

B-1: Upon  $Z_1^{n_1}, u'_1$ , Bob computes and sends  $v_1 = \pi_n(B, r_B, Z_1^{n_1}, u'_1)$  to Alice over the noiseless channel. Through Oscar, Alice will receive  $v'_1$ .

$\vdots$

A- $i$ : Upon  $v'_{i-1}$ , Alice computes

$$(X_i^{n_i}, u_i) = \pi_n(A, S, r_A, v'_1 | v'_2 | \dots | v'_{i-1}).$$

He sends  $X_i^{n_i}$  over channel  $W_1$  and  $u_i$  over the noiseless channel. Oscar will see  $X_i^{n_i}, Z_i^{n_i}$  and  $u_i$ . He can modify  $u_i$  to  $u'_i$ . Bob will receive  $Z_i^{n_i}$  from channel  $W_1$  and  $u'_i$  from the noiseless channel.

B- $i$ : Upon  $Z_i^{n_i}, u'_i$ , Bob computes and sends

$$v_i = \pi_n(B, r_B, Z_1^{n_1} | u'_1 | Z_2^{n_2} | u'_2 | \dots | Z_i^{n_i} | u'_i)$$

to Alice over the noiseless channel, which, through Oscar, becomes  $v'_i$ .

$\vdots$

B- $\nu$ : Upon  $Z_\nu^{n_\nu}, u'_\nu$ , Bob computes

$$S' = \pi_n(B, r_B, Z_1^{n_1} | u'_1 | Z_2^{n_2} | u'_2 | \dots | Z_\nu^{n_\nu} | u'_\nu)$$

for  $S' \in \mathcal{S} \cup \{\perp\}$ , where  $S' = \perp$  means that he rejects the authentication while  $S' \neq \perp$  means that he agrees that  $S'$  is authenticated from Alice.

If Alice (or Bob) detects any inconsistency before the protocol completion, she (or he) can reject and abort the execution immediately.

2) *Security model*: The security model is described in terms of two attacks. In a type I attack, Oscar can change the messages over the two-way noiseless channel between Alice and Bob. He succeeds if Bob accepts a source state that is different from Alice's input. In a type II attack, Oscar can impersonate Alice to authenticate a source state using  $W_2$  and a noiseless channel. He succeeds if Bob accepts his authentication. The formal description is as follows.

*Admissible Attacks*:

- I. During the execution of  $\pi_n$  between Alice and Bob, Oscar can see  $(X_i^{n_i}, Z_i^{n_i}, u_i)$  from Alice and  $v_i$  from Bob. He can modify  $u_i$  to any  $u'_i$  and  $v_i$  to any  $v'_i$ . He succeeds if Bob outputs  $S' \in \{S, \perp\}$ .
- II. Oscar can impersonate Alice to execute  $\pi_n$  with Bob, except that the noisy channel  $W_1$  is replaced by  $W_2$ . He succeeds in this attack if Bob outputs  $S' \neq \perp$ .

We use *succ* to denote a success event in a type I or II attack.

*Security definition*: In this paper, we assume by default that an honest Alice (or Bob) follows the protocol with a random input that is a uniformly random binary string. However, we also consider an honest Alice or Bob who follows the protocol specification with some  $r \in \{0, 1\}^*$  as the random input. In this case, we call her (or him) an *admissible* user. Now the security consists of two properties: correctness and authentication. The correctness requires that if an admissible Alice authenticates  $S$  to Bob when no attack is performed, Bob should output  $S' = S$ . The authentication requires that Oscar will never succeed in a type I or II attack.

*Definition 4*: An authentication protocol  $\pi_n$  for source  $S$  is *secure* if it satisfies two properties.

- **Correctness.** For any admissible Alice, Bob outputs  $S' \neq S$  only negligibly (in  $n$ ) if no attack is performed.
- **Authentication.** Under type I and type II attacks,  $\Pr(\text{succ})$  is negligible in  $n$ .

Note that here we require the error probability to be *negligible* (see Section II) as this is the widely accepted quantity for a probabilistic event that is unlikely to occur.

3) *Authentication rate and authentication capacity*: We regard the noisy channel as an expensive resource and the noiseless channel as a cheap source. So we are interested in maximizing the efficiency of channel  $W_1$  and define the *authentication rate* of  $\pi_n$  as the ratio  $\frac{\log |S|}{n}$ . The authentication model with  $(W_1, W_2)$  has an *authentication capacity*  $C_a$ , if any authenticate rate  $r < C_a$  can be achieved by a certain protocol  $\pi_n$  while any protocol with an authentication rate  $r > C_a$  is insecure.

#### IV. OUR AUTHENTICATION PROTOCOL

This section extends the 3-round authentication protocol in [17]. The number  $n$  of channel  $W_1$  uses in the protocol of [17] satisfies  $n \geq \frac{\log \log |S|}{C}$ , where  $C$  is the shannon capacity of  $W_1$  and  $S$  is the source space. In this section, we improve the protocol such that  $n$  does not depend on  $|S|$  but with the price that the round complexity is  $\log^* |S| - \log^* n + 4$ . Under our result, the authentication rate  $\frac{\log |S|}{n}$  is proportional to  $\log |S|$ .

The 3-round protocol in [17] is based on a set system  $(S, \mathcal{B}_1, \dots, \mathcal{B}_b)$ . The idea is as follows. Alice first sends the

source state  $S$  to Bob noiselessly. Bob then finds all possible  $i$ 's such that  $S \in \mathcal{B}_i$  and picks a random  $\mathcal{B}_j$  among them and sends  $j$  to Alice noiselessly. Finally, Alice sends  $j$  via DMC  $W_1$  to Bob. The construction is designed such that if  $S$  is modified to  $S'$  by Oscar, then a successful type I attack implies  $S', S \in \mathcal{B}_j$ , which is unlikely due to the property of the set system.

Our new protocol stems from [17] with the following idea. Essentially, Alice still attempts to authenticate  $S$  using a set system  $(S, \mathcal{B}_1, \dots, \mathcal{B}_b)$ . However, she does not send  $j$  over  $W_1$ . Instead, he regards  $j$  as a new source state in a new but smaller source space  $S' = [b]$  and attempts to use a smaller set system  $(S', \mathcal{B}_1, \dots, \mathcal{B}_{b'})$  to authenticate  $j$ . It is important to notice that  $b$  has the order of  $\log |S|$  by Lemma 5. Similarly,  $b'$  has the order of  $\log b$ , which in turn has the order of  $\log \log |S|$ . So to authenticate  $j$ , Alice now only needs to send a DMC message from a domain of  $b' = \log \log |S|$  (instead of a domain of size  $b = \log |S|$ ). That is, two iterations on the protocol of [17] allow to decrease DMC message to the log size. Continuing with this idea, if we iterate the protocol [17] for  $L$  times, then conceivably the DMC message will reduce to a domain size of  $\log^{(L)} |S|$ . Thus, if the DMC message length is  $n$ , then it suffices to iterate the protocol in [17] for  $\log^* |S| - \log^* n + O(1)$  times (using the fact  $\log^* m = L + \log^*(\log^{(L)} m)$  for any  $m$  and  $L \leq \log^* m$ ). This gives our desired result. In the following, we implement this idea rigorously.

##### A. The construction

For any  $R < C$  ( $C$  is the shannon capacity over  $W_1$ ), Shannon capacity theorem tells us that there exists a channel code  $\mathcal{C} = \{C_1, \dots, C_{2^{n'R}}\} \subseteq \mathcal{X}^{n'}$  that has a maximum error probability  $\delta_{n'} \rightarrow 0$  exponentially with  $n'$  (see [13]). Assume  $\mathcal{C}$  has an encoding  $f_{n'}$  and a decoding  $g_{n'}$ .

For  $v_1 \in \mathbb{N}$ , let  $\mathcal{S} = [v_1]$  be the source space. Take  $\epsilon = 2^{-\beta_1 n'}$  for some  $\beta_1 \in (0, R/4)$ . Let  $\phi$  be the minimal even  $t$  s.t.  $\log^{(t)} v_1 \leq \beta_2 n' + \sqrt{n'}$  for some  $\beta_2 \in (0, R - 4\beta_1)$ . Let  $v_{j+1} = \lfloor \frac{2^{\phi-j+8}}{\epsilon^4} \log v_j \rfloor$  for each  $j < \phi$ . By Lemma 5, there exists a  $(v_j, v_{j+1}, 2^{-.25(\phi-j)-2}\epsilon v_{j+1}, 2^{-.5(\phi-j)-2}\epsilon^2 v_{j+1})$ -set system, which we denote by  $\mathbb{S}_j = (\mathcal{S}_j, \mathcal{B}_{j,1}, \dots, \mathcal{B}_{j,v_{j+1}})$  with  $\mathcal{S}_j = [v_j]$ . Assume Alice wants to authenticate source state  $s \in \mathcal{S}$ . The protocol is described in Fig. 2, where we assume  $W_1(\cdot|a) \notin \text{Cov}(W_2)$  for some  $a \in \mathcal{X}$ .

##### B. Security analysis

Now we analyze the security of our new protocol. Before this, we first prove the following preparation lemma.

*Lemma 7*: Let  $0 < \delta < 1, k \in \mathbb{N}, v_1 > 0$  with  $\log^{(k)} v_1 \geq 3$ . If  $v_{j+1} \leq \frac{2^{k-j}}{\delta} \log v_j$  for  $1 \leq j \leq k$ , then

$$v_{j+1} < \frac{2^{k-j} \log^{(j)} v_1}{\delta} + \frac{2^{k-(j-1)}}{\delta} \log\left(\frac{2^{k-(j-1)}}{\delta}\right).$$

**Proof.** The conclusion holds for the initial case  $j = 0$  automatically. Assume it holds for case  $j - 1$ . Consider case  $j$ . Let  $\alpha_i = \frac{2^{k-(i-1)}}{\delta} \log\left(\frac{2^{k-(i-1)}}{\delta}\right)$  for any  $i$ . By induction,

0. Let  $s_1 = s, s_0 = 1, L_{0,i} = \{1\}$  for any  $i \in [v_1]$ .
1. For  $\ell = 1$  to  $\phi$ , do the following. Let  $\mathcal{P}_1 = \mathcal{P}_3 = \dots = \text{Alice}$  and  $\mathcal{P}_2 = \mathcal{P}_4 = \dots = \text{Bob}$ .

- a.  $\mathcal{P}_\ell$  sends  $s_\ell$  to  $\mathcal{P}_{\ell+1}$  over the noiseless channel, which, through Oscar, arrives at  $\mathcal{P}_{\ell+1}$  as  $s'_\ell$ .
- b. Upon  $s'_\ell$ ,  $\mathcal{P}_{\ell+1}$  checks if  $s_{\ell-1} \in \mathcal{B}_{\ell-1, s'_\ell}$ . If not, (s)he rejects; otherwise, (s)he determines

$$L_\ell = \{\mathcal{B}_{\ell,i} \mid s'_\ell \in \mathcal{B}_{\ell,i}, i \in [v_{\ell+1}]\}.$$

Assume  $L_\ell = \{\mathcal{B}_{\ell,i_1}, \dots, \mathcal{B}_{\ell,i_r}\}$  ( $r$  might vary with  $s'_\ell$ ). If  $\ell < \phi$ , (s)he takes  $s_{\ell+1}$  from  $\{i_1, i_2, \dots, i_r\}$  uniformly randomly and proceeds to iteration  $\ell + 1$ ; otherwise ( $\ell = \phi$ , even,  $\mathcal{P}_{\ell+1} = \text{Alice}$ ), she goes to step 2.

2. Alice sends  $C_{s'_\phi}^* = a^k |C_{s'_\phi}$  over  $W_1$  for  $k = \sqrt{n'}$ .
3. Upon  $Z^{n'+k}$ , Bob checks if

$$|T_{Z^k}(u) - W_1(u|a)| \leq \frac{\gamma}{2|\mathcal{Z}|}$$

for all  $u \in \mathcal{Z}$ , where  $\gamma = \Delta(W_1(\cdot|a); \text{Cov}(W_2))$ . If no, he rejects; otherwise, he accepts if and only if  $Z_{k+1}^{k+n'}$  is decoded to  $s_\phi$ .

Fig. 2. Our authentication protocol SetAuth\*

$$\begin{aligned} v_{j+1} &< \frac{2^{k-j}}{\delta} \log\left(\frac{2^{k-(j-1)} \log^{(j-1)} v_1}{\delta} + \alpha_{j-1}\right) \\ &\leq \frac{2^{k-j}}{\delta} \log\left(\frac{2^{k-(j-1)} \log^{(j-1)} v_1}{\delta}\right) + \frac{\alpha_{j-1}}{2 \ln 2 \cdot \log^{(j-1)} v_1} \\ &\leq \frac{2^{k-j}}{\delta} \log^{(j)} v_1 + \frac{2^{k-j}}{\delta} \log\left(\frac{2^{k-(j-1)}}{\delta}\right) + \frac{\alpha_{j-1}}{\log^{(j-1)} v_1} \\ &\stackrel{(*)}{\leq} \frac{2^{k-j}}{\delta} \log^{(j)} v_1 + 2 * \frac{2^{k-j}}{\delta} \log\left(\frac{2^{k-(j-1)}}{\delta}\right) \\ &= \frac{2^{k-j}}{\delta} \log^{(j)} v_1 + \alpha_j, \end{aligned}$$

where inequality (\*) uses the fact that  $\log^{(j-1)} v_1 \geq \log^{(k-1)} v_1 \geq 2^3$  and that  $4x \log x \geq 2x \log(2x)$  for  $x = \frac{2^{k-(j-1)}}{\delta} \geq 2$ .  $\square$

Applying the lemma to our construction with  $\delta = 2^{-8} \epsilon^4$  and  $k = \phi - 1$ , we have

*Corollary 1:* Keep notions as in protocol SetAuth\*. Then,

$$v_\phi < 2^{9+4\beta n'} \left( \log^{(\phi-1)} v_1 + 20 + 8\beta n' \right). \quad (4)$$

*Theorem 1:* If  $\text{Cov}(W_1) \not\subseteq \text{Cov}(W_2)$  and  $\dim W_1 > 1$ , then SetAuth\* is a  $2^{-\xi \sqrt{n}}$ -secure authentication protocol for a constant  $\xi > 0$  with round complexity at most  $\log^* v_1 - \log^* n + 4$ , where  $n = n' + \sqrt{n'}$  is the number of channel  $W_1$  uses which does not depend on  $v_1$ .

**Proof.** *Correctness.* When Oscar does not involve in the attack,  $s_\ell = s'_\ell$  for all  $\ell$ . From Corollary 1 and  $4\beta_1 + \beta_2 < R$ , we know that  $v_\phi < 2^{n'R}$  when  $n'$  large enough. Since  $s_\phi$  is taken from  $\mathcal{S}_\phi$  (of size  $v_\phi$ ), Bob will decode  $C_{s'_\phi}$  to  $s'_\phi$  with an exponentially small error probability, by the assumption of  $\mathcal{C}$ . In addition, by Lemma 1,  $|T_{Z^k}(u) - W_1(u|a)| \leq \frac{\gamma}{2|\mathcal{Z}|}$  for all  $u \in \mathcal{Z}$  is violated with an exponentially small probability too. The correctness follows.

*Authentication.* By the authentication model, there are two types of attacks.

**Type-I.** Oscar revises messages over the noiseless channel between Alice and Bob such that  $s_1 \neq s'_1$ .

**Type-II.** Oscar plays the role of Alice to interact with Bob to authenticate  $\tilde{s}$ , where assume that the message in the iteration  $\ell$  in step 1 is  $\tilde{s}_\ell$ . Further, at step 2, we assume Oscar sends  $\tilde{C}^*$  over the channel  $W_2$  to Bob.

For a type I attack, the success probability is bounded by  $P(\text{succ}|s'_\phi \neq s_\phi) + P(\text{succ}|s'_\phi = s_\phi)$ . Note that  $\text{succ}$  event implies the decoding result  $g_{n'}(Z_{k+1}^{k+n'}) = s_\phi$ . By correctness of code  $\mathcal{C}$ ,  $P(g_{n'}(Z_{k+1}^{k+n'}) = s'_\phi) > 1 - 2^{-n'\alpha}$  for some  $\alpha > 0$ . So  $P(\text{succ}|s'_\phi \neq s_\phi) \leq 2^{-n'\alpha}$ . We thus focus on the case  $s'_\phi = s_\phi$ . In this case, as  $s'_1 \neq s_1$ , there must exist  $j < \phi$  such that  $s'_j \neq s_j$  but  $s'_{j+1} = s_{j+1}$ . In this case, notice that  $P_{j+2}$  will verify whether  $s_j \in \mathcal{B}_{j,s'_{j+1}}$ . We now bound the probability for this to hold. First, observe that the time order for  $s_j, s'_j, s_{j+1} = s'_{j+1}$  is as follows:  $P_j$  generates  $s_j$ ; then, Oscar revises it to  $s'_j$ ; next, upon  $s'_j$ ,  $P_{j+1}$  generates  $s_{j+1}$ ; finally,  $P_{j+2}(= P_j)$  receives  $s'_{j+1} = s_{j+1}$ . Thus,  $s_{j+1} = s'_{j+1}$  is selected after  $s_j$  and  $s'_j$  have been fixed. By the definition of  $s_{j+1}$ , it holds that  $s'_j \in \mathcal{B}_{j,s_{j+1}}$ . Since  $P_{j+2}$  will verify  $s_j \in \mathcal{B}_{j,s'_{j+1}}$ , it follows that a successful attack implies  $s_j, s'_j \in \mathcal{B}_{j,s_{j+1}}$ . However, as  $s_{j+1}$  is uniformly randomly from  $\{i_1, \dots, i_r\}$ , this probability is at most  $2^{-.25(\phi-j)\epsilon}$ , by the property of the set system  $\mathbb{S}_j$ . Since  $j$  can take any value from 1 to  $\phi - 1$ , it follows that

$$P(\text{succ}|s'_\phi = s_\phi) \leq \sum_{j=1}^{\phi-1} 2^{-.25(\phi-j)\epsilon} < \frac{2^{-.25\epsilon}}{1 - 2^{-.25}} < 6\epsilon.$$

Hence, a type I attack succeeds with probability at most  $2^{-n'\alpha} + 6\epsilon$ , which is exponentially small as  $\epsilon = 2^{-\beta n'}$ .

For a type II attack, assume Bob receives  $Z^{n'+k}$ . We claim

$$P_{Z^k} \left( |T_{Z^k}(u) - W_1(u|a)| \leq \frac{\gamma}{2|\mathcal{Z}|}, \forall u \right) \leq 2e^{-\frac{k\gamma^2}{8|\mathcal{Z}|^2}}.$$

Otherwise, by Lemma 2,

$$\Delta(W_1(\cdot|a); \text{Cov}(W_2)) \leq \gamma/2 + \gamma/4 < \gamma.$$

This is impossible, as  $\Delta(W_1(\cdot|a); \text{Cov}(W_2)) = \gamma$ . This completes the proof of the authentication property by defining  $\xi < \frac{\gamma^2}{8|\mathcal{Z}|^2}$ .

Finally, as  $\log^* v_1 = \phi + \log^*(\log^{(\phi)} v_1)$  and  $\log \log(\beta_2 n) < \log^{(\phi)} v_1 \leq n$  by the definition of  $\phi$ , we have  $\phi \leq \log^* v_1 - \log^* n + 3$  (using  $2^{\beta_2 n} \geq n$ ) for  $n$  large enough. This gives the round complexity.  $\blacksquare$

## V. LOWER BOUND ON ROUND COMPLEXITY

In this section, we prove a lower bound on the round complexity of an authentication protocol in our model. Our strategy is to reduce the problem to a special class of protocols and then bound the round complexity of the latter.

Toward this, we define  $\Sigma_1$  to be the set of authentication protocols in our model such that the DMC message over  $W_1$  is sent only in the final flow and the final flow has no message over the noiseless channel.

In the following, we show that if there is an  $L$ -round secure authentication protocol in our model, there exists a secure  $L'$ -round protocol in  $\Sigma_1$  with  $L' \leq L + 2$ . Our idea is that we can move each DMC message  $X^{n_i}$  in the original protocol to the noiseless channel of the same flow and in addition also send  $X^{n_i}$  over DMC  $W_1$  in the final flow. This modification needs to be careful: the original protocol could use the DMC output  $Y^{n_i}$  right after Bob has received it while the modified protocol only has the noiseless version  $X^{n_i}$  (instead of  $Y^{n_i}$ ). Fortunately, this can be fixed by permitting Bob to simulate  $Y^{n_i}$  (letting  $X^{m_i}$  go through a statistical model that has the same characteristics as channel  $W_1$ ), where  $X^{m_i}$  is the received version of  $X^{n_i}$  by Bob over the noiseless channel. However, this causes a new problem: it is possible that  $X^{m_i} \neq X^{n_i}$ . To overcome this, we actually send  $X^{n_i}$  in the final flow using an error-correcting code, through which Bob can obtain  $X^{n_i}$  with high probability. In addition,  $X^{n_i}$  is coded such that if  $X^{m_i} \neq X^{n_i}$ , then the change can be detected. The formal result is as follows.

**Lemma 8:** If there exists an  $L$ -round  $\epsilon$ -secure authentication protocol  $\pi$  in our model, then there exists an  $L'$ -round  $(\epsilon + 2^{-\beta n'})$ -secure authentication protocol  $\pi' \in \Sigma_1$  with  $n' = \mu n$  for  $L' \leq L + 2$  and some constants  $\beta > 0, \mu > 0$ , where  $n', n$  are respectively the numbers of channel  $W_1$  uses in  $\pi', \pi$ .

**Proof.** Let  $\pi$  be an  $L$ -round  $\epsilon$ -secure authentication protocol in our model. We construct an  $L'$ -round  $(\epsilon + 2^{-\beta n'})$ -secure authentication protocol  $\pi'$  from  $\pi$  as follows. W.L.O.G., assume  $W_1(\cdot|a) \notin \text{Cov}(W_2)$  (by [17], a necessary condition for  $\epsilon$ -secure authentication is  $\text{Cov}(W_1) \not\subseteq \text{Cov}(W_2)$ ).

- i. Alice follows  $\pi$ , except that whenever she needs to send  $F$  over  $W_1$ , she instead sends it over the noiseless channel.
- ii. Bob follows  $\pi$ , except that whenever he receives  $F'$  over the noiseless channel (the received version of  $F$ , where  $F$  is supposedly sent over DMC  $W_1$  in  $\pi$ ), she lets it go through a simulated  $W_1$  and regards the output as the DMC output in  $\pi$  and proceeds normally according to  $\pi$ .
- iii. If the  $L$ th flow in  $\pi$  is from Alice to Bob, then Bob sends 0 as the  $(L+1)$ th flow in  $\pi'$  and the  $(L+2)$ th flow will be the final flow; otherwise, the  $(L+1)$ th flow will be the final flow. In any case, the final flow in  $\pi'$  is from Alice to Bob and defined as follows. Let  $(F_1, \dots, F_L)$  be the list of messages that are sent over DMC  $W_1$  in  $\pi$ . Since  $\pi$  uses  $W_1$  for  $n$  times, it follows  $F^L \in \mathcal{X}^n$ . Let  $\bar{n} = \frac{2n \log |\mathcal{X}|}{C}$ , where  $C$  is the Shannon capacity of  $W_1$  ( $C > 0$  is implied by the necessary condition  $\dim W_1 > 1$  [17]). By Shannon capacity theorem, there exists a code  $\mathcal{C} \subseteq \mathcal{X}^{\bar{n}}$  over channel  $W_1$  for source  $\mathcal{M} = \mathcal{X}^n$  that has an exponentially small error probability (say,  $2^{-\alpha \bar{n}}$  for some  $\alpha > 0$ ). Alice encodes  $(F_1, \dots, F_L)$  to  $X^{\bar{n}} \in \mathcal{C}$  and sends  $a^{\bar{n}} X^{\bar{n}}$  over DMC  $W_1$  in the final flow of  $\pi'$ .
- iv. Let  $Y^{2\bar{n}}$  be the received vector in the final flow  $\pi'$  for  $a^{\bar{n}} X^{\bar{n}}$  over channel  $W_1$ . Bob will accept the authentication if and only if
  - the original verifications in  $\pi$  are satisfied;
  - $Y_{\bar{n}+1}^{2\bar{n}}$  decodes to  $F'^L$  (the received version of  $F^L$  over the noiseless channel by Bob in  $\pi'$ );

$$- Y^{\bar{n}} \in \mathbf{T}_{[W_1].s\gamma}^{\bar{n}}(a^{\bar{n}}) \text{ for } \gamma = \Delta(W_1(\cdot|a), \text{Cov}(W_2)).$$

This completes the description of  $\pi'$ .

Now we analyze the security of  $\pi'$ . Consider a type I attack first. For any Oscar' against  $\pi'$  (executed between Alice' and Bob'), we construct Oscar against  $\pi$  (executed between Alice and Bob). The strategy of Oscar is to maintain a simulated Alice' and Bob' to execute  $\pi'$  with Oscar' against it and then mimic the attack strategy of Oscar' to attack  $\pi$ . Toward this, the simulation of Alice' and Bob' will rely on the view of Oscar in the execution of  $\pi$ . Details follow.

- When Alice (or Bob) in  $\pi$  sends  $M$  over the noiseless channel, Oscar lets Alice' (or Bob') do the same thing in  $\pi'$  and also lets Oscar' know  $M$ . In addition, whenever Alice sends  $F_i$  over channel  $W_1$ , Oscar lets Alice' in  $\pi'$  sends  $F_i$  to Bob' over the noiseless channel.
- When Oscar' (against  $\pi'$ ) changes  $M$  to  $M'$  before the delivery, Oscar (against  $\pi$ ) does the same thing. When Oscar' changes  $F_i$  to  $F'_i$ , Oscar aborts immediately; otherwise, Oscar' will deliver  $F_i$  without a change (recall that Alice in  $\pi$  has sent  $F_i$  over  $W_1$ ). If Bob in  $\pi$  receives  $\bar{Y}^{n_i}$  over  $W_1$  (when Alice sends  $F_i$ ), then Oscar lets Bob' use  $\bar{Y}^{n_i}$  as the simulated output of  $W_1$  with input  $F_i$ . Note this  $\bar{Y}^{n_i}$  has the same distribution as the simulated output by Bob' in  $\pi'$  as they are both according to the statistic model  $W_1$ .
- In the last round of  $\pi'$ , Oscar simulates Alice' and Bob' to act normally. He lets Oscar' know the input  $a^{\bar{n}} X^{\bar{n}}$  and output  $Y^{2\bar{n}}$  of DMC  $W_1$ .

Denote the above attack of Oscar by  $\Gamma'$ . Note that the view of Oscar' in  $\Gamma'$  is according to the distribution in a real attack. It suffices to bound the success event (denoted by  $\text{succ}'$ ) of Oscar' in  $\Gamma'$ . Thus,

$$P(\text{succ}') = P(\text{succ}', F_i \neq F'_i, \exists i) + P(\text{succ}', F^L = F'^L).$$

Note if  $(F_1, \dots, F_L) \neq (F'_1, \dots, F'_L)$ ,  $\text{succ}'$  implies a decoding error for  $Y_{\bar{n}+1}^{2\bar{n}}$ , which is bounded by  $2^{-\alpha \bar{n}}$  for some  $\alpha > 0$  (by the classic random coding result as the information rate is less than  $\frac{\log |\mathcal{X}|^n}{\bar{n}} \leq C/2 < C$ ). Further, when  $(F_1, \dots, F_L) = (F'_1, \dots, F'_L)$ , the success of Oscar' in  $\pi'$  implies the success of Oscar in  $\pi$ , which is bounded by  $\epsilon$  due to our assumption for  $\pi$ . Hence,  $P(\text{succ}') \leq 2^{-\alpha \bar{n}} + \epsilon$ .

Then, we consider type II attack. In this case, it is similar to the analysis of type II attack in SetAuth\* that the success probability of the attacker is bounded by  $2e^{-\frac{\bar{n}\gamma^2}{8|\mathcal{Z}|^2}}$ .

As a summary, the success probability of type I and II attacks is bounded by  $\epsilon' = \epsilon + 2^{-\alpha \bar{n}} + 2e^{-\frac{\bar{n}\gamma^2}{8|\mathcal{Z}|^2}}$ . Finally, the number of channel  $W_1$  uses in  $\pi'$  is  $n' = 2\bar{n} = \frac{4n \log |\mathcal{X}|}{C}$ . Thus, a value is negligible in  $n'$  if and only if it is negligible in  $n$ . Thus,  $\pi'$  is  $\epsilon'$ -secure under parameter  $n'$ . This completes our proof. ■

In the following, we show that we can always assume the first flow of the protocol is the source state  $S$  over the noiseless channel from Alice. The idea is that the source state is not confidential and hence the authentication property does not depend on its secrecy. Thus, if it is not sent in the first flow, then we can prepend it to the protocol.

**Lemma 9:** Let  $\pi$  be an  $L$ -round  $\epsilon$ -secure authentication protocol in our model for source space  $\mathcal{S}$ . Let  $\pi'$  be an authentication protocol obtained from  $\pi$  as follows:

- The first flow of  $\pi'$  is the source state  $S$  over the noiseless channel from Alice;
- If the first flow in  $\pi$  is from Alice, then the second flow of  $\pi'$  is a constant message 0 over the noiseless channel from Bob;
- After the preliminary flow(s) above, Alice and Bob start to execute  $\pi$  normally with  $S$  as Alice's input in  $\pi$ .

Then,  $\pi'$  is an  $L'$ -round  $\epsilon$ -secure authentication in our model with  $L' \leq L + 2$ .

**Proof.** If there exists an Oscar' against  $\pi'$ , we present an Oscar against  $\pi$ . We describe Oscar for type I and II attacks as follows. Assume  $\pi$  is run between Alice and Bob and  $\pi'$  is run between Alice' and Bob'. The strategy of Oscar is to simulate Alice' and Bob' and run Oscar' against the execution of  $\pi'$ . W.L.O.G., assume  $\pi$  starts with Alice.

For a type I attack, Oscar does as follows.

- When Oscar' invokes Alice' (in  $\pi'$ ) to authenticate  $S$  to Bob', Oscar simulates Alice' with input  $S$  and sends  $S$  to Bob', which through Oscar' will be delivered to Bob' as  $S'$ . Bob' will then send 0 to Alice', which we assume to arrive at Alice' as 0 (otherwise, Alice' simply rejects). In this case, Oscar invokes Alice (in  $\pi$ ) with input  $S$ . Further, Oscar simulates Alice' and Bob' to start  $\pi$  (as a subprotocol of  $\pi'$ ) with input  $S$ , by strictly following the flows between Alice and Bob. Details follow.
- Whenever Alice (or Bob) sends a message  $C$  to Bob (or Alice) noiselessly, Oscar simulates Alice' (or Bob') to send  $C$  to Bob' (or Alice') noiselessly as well.
- Whenever Oscar' delivers a message  $M'$  to Bob' (or Alice'), Oscar delivers  $M'$  to Bob (or Alice) in  $\pi$  as well.
- Whenever Alice sends a message  $X^t$  to Bob over  $W_1$ , Oscar simulates Alice' to send  $X^t$  over (virtual)  $W_1$  as well and informs Oscar' about this. When  $X^t$  in  $\pi$  arrives at Bob as  $Y^t$ , Oscar delivers  $Y^t$  to Bob' as the output of  $W_1$  and also notifies  $Y^t$  to Oscar'.

From the description of Oscar, the view of Oscar' is distributed according to the real attack. Also when Oscar' successfully authenticates  $S' \neq S$  to Bob', Oscar do so to Bob as well, as the execution of  $\pi$  between Alice' and Bob' and the execution of  $\pi$  between Alice and Bob are identical. Especially, Bob' accepts  $S'$  if and only if Bob accepts  $S'$ . Thus, Oscar has the same success probability as Oscar'.

For type II attack, Oscar's strategy is similar, omitted. ■

In the following, we will prove our lower bound on the round complexity. Our idea is as follows. By Lemma 8 and Lemma 9, we only need to consider a protocol  $\pi$  whose first flow is the source state  $S$  over the noiseless channel from Alice and the final flow consists of only a DMC message from Alice, which also is the only flow that has a DMC message. We first consider such a protocol of 3-round and show that its source space must be bounded by  $2^{1+2^{|\mathcal{X}|^n+1}}$ . If  $u^{j-1}$  is the first  $j-1$  flows, then we define  $\mathcal{M}_j(u^{j-1})$  to be the set of all possible messages in the  $j$ th flow. For convenience, we regard **reject** is also as a possible message. It is immediate

that  $\mathcal{M}_3(u^2) \subseteq \mathcal{X}^n \cup \{\text{reject}\}$ . If we sort  $\mathcal{X}^n \cup \{\text{reject}\}$  in any fixed order,  $\mathcal{M}_3(u^2)$  can be represented by a binary vector  $\mathbf{D}(u^2) = (d_0, \dots, d_{|\mathcal{X}|^n})$ , where  $d_i = 1$  if and only if  $\mathcal{M}_3(u^2)$  contains the  $i$ th element in  $\mathcal{X}^n \cup \{\text{reject}\}$ . Thus, each  $\mathbf{D}(u^2)$  must be one of these  $2^{|\mathcal{X}|^n+1}$  binary vectors. Now we consider the case where the second flow  $u_2$  is always 0 (constant). In this case, if  $|\mathcal{S}| > 2^{|\mathcal{X}|^n+1}$ , then there must exist  $u_1, \bar{u}_1$  such that  $\mathbf{D}(u_1 0) = \mathbf{D}(\bar{u}_1 0)$ . Then, Oscar can attack  $\pi$  as follows. He first requests Alice to authenticate  $u_1$  and then modifies the first flow  $u_1$  to  $\bar{u}_1$  but keeps other flows unchanged. Under this attack, Oscar is admissible, as  $u_3 \in \mathcal{M}_3(\bar{u}_1 0)$  from  $\mathbf{D}(u_1 0) = \mathbf{D}(\bar{u}_1 0)$ . By the correctness of the authentication protocol, Bob will accept  $\bar{u}_1$  and hence Oscar succeeds. This contradicts the authentication property. Thus, we must have that  $|\mathcal{S}| \leq 2^{|\mathcal{X}|^n+1}$ . Our foregoing argument is based on the restriction that  $u_2$  is a constant, which is of course not true usually. However, for the general case, we might still wish to use a certain variant of this strategy. Specifically, we may try to define  $\mathbf{D}(u)$  such that if the number of possible vectors  $\mathbf{D}(u)$  is less than  $|\mathcal{S}|$ , then there must exist two source states  $u_1, \bar{u}_1$  which share the same possible choices for the second flow and the third flow. In this case, the above attack can go through. Toward this, we use  $\mathbb{D}_2$  to denote all possible  $\mathbf{D}(u^2)$  and define  $\mathbf{D}(u_1) = (d_0, \dots, d_{|\mathbb{D}_2|})$ , where  $d_i = 1$  if and only if there exists  $u_2$  such that  $\mathbf{D}(u^2)$  is the  $i$ th element in  $\mathbb{D}_2 \cup \{\text{reject}\}$ . Notice that  $|\mathbb{D}_2| \leq 2^{|\mathcal{X}|^n+1}$ . Hence, under our treatment, an variant of Oscar's attack above succeeds if the number of all possible  $\mathbf{D}(u)$  is less than  $|\mathcal{S}|$  (which is guaranteed if  $|\mathcal{S}| > 2^{1+2^{|\mathcal{X}|^n+1}}$ , or roughly  $\log^{(2)} |\mathcal{S}| > |\mathcal{X}|^n$ ). So the authentication property necessarily implies  $\log^{(2)} |\mathcal{S}| \leq |\mathcal{X}|^n$  (roughly). For a general  $L$ -round protocol, we can generalize the above idea to show that  $\log^{(L-1)} |\mathcal{S}| \leq |\mathcal{X}|^n$  (roughly). From  $L-1 = \log^* |\mathcal{S}| - \log^*(\log^{(L-1)} |\mathcal{S}|)$ , this gives  $L-1 \geq \log^* |\mathcal{S}| - \log^*(|\mathcal{X}|^n)$ , which is basically our desired lower bound on the round complexity. We now implement the above idea rigorously. We start with a claim.

**Claim 1.** If  $D_L \geq 3$  and  $D_i \leq 2^{1+D_{i+1}}$  for any  $i = 1, \dots, L-1$ , then  $\log^{(L)} D_1 \leq 1 + \log D_L$ .

**Proof.** It suffices to prove the bound when  $D_i = 2^{1+D_{i+1}}$  for each  $j$ , as in this case  $D_1$  achieves the largest possible value. Notice that if  $\log A_1 \leq b + A_2$  for  $A_2 \geq 3$ , then

$$\log^{(2)} A_1 \leq \log A_2 + \log(1 + \frac{b}{A_2}) \leq \log A_2 + \frac{b}{2}. \quad (5)$$

Hence, from  $\log D_j = 1 + D_{j+1}$  and  $D_{j+1} \geq 3$  (as  $D_L \geq 3$ ),

$$\log^{(2)} D_1 \leq \log D_2 + \frac{1}{2} \leq D_3 + 1 + \frac{1}{2}$$

Using Eq. (5) again, we have

$$\log^{(3)} D_1 \leq \log D_3 + (1 + \frac{1}{2})/2 \leq D_4 + 1 + \frac{1}{2} + \frac{1}{2^2}.$$

Continuing this evaluation, we have

$$\begin{aligned} \log^{(L)} D_1 &\leq \log D_L + (1 + \frac{1}{2} + \dots + \frac{1}{2^{L-1}})/2 \\ &\leq \log D_L + 1. \end{aligned}$$

This completes the proof. ■

We now formally present our theorem.

**Theorem 2:** Let  $\pi$  be an  $L$ -round  $\epsilon$ -secure authentication protocol for source space  $\mathcal{S}$ . Then  $L \geq \log^* |\mathcal{S}| - \log^* n - 5$ , where  $n$  is the number of channel  $W_1$  uses.

**Proof.** We first prove the theorem for  $\pi$  with the following restrictions: (a) the first flow is the source state  $S$  over the noiseless channel from Alice; (b) the final flow is a DMC message over  $W_1$  from Alice and a DMC message is only sent in the final flow.

If the first  $j-1$  flows are  $u^{j-1}$ , we define  $\mathcal{M}_j(u^{j-1})$  to be the set of possible messages in the  $j$ th flow by  $U \in \{\text{Alice}, \text{Bob}\}$ . Formally,  $u_j \in \mathcal{M}_j(u^{j-1})$  if and only if there exists random tape  $r$  such that the list of messages of  $U$  with random tap  $r$  (given the list of incoming message  $u_{j-1}, u_{j-3}, \dots$ ) are  $u_j, u_{j-2}, \dots$ . For convenience, if  $U$  rejects (given  $u^{j-1}$ ), we regard it as  $u_j = \perp$ , where  $\perp$  is different from any legal message flow. When  $U$  rejects, (s)he aborts the execution immediately. Since  $\perp$  is not an actual message flow,  $u_j = \perp$  will be never delivered. Hence, when  $U$  has the view of  $u^{j-1}$  on the first  $j-1$  flows and is going to compute  $u_j$ , then implicitly  $u_i \neq \perp$  for any  $i \leq j-1$ .

By the definition of  $n$ , we have  $u_L \in \mathcal{X}^n \cup \{\perp\}$ . If  $u^{L-1}$  is the first  $L-1$  flows, then we define a  $(|\mathcal{X}|^n + 1)$ -dimensional binary vector  $\mathbf{D}(u^{L-1}) = (d_0, d_1, \dots, d_{|\mathcal{X}|^n})$ , where  $d_t = 1$  if and only if the  $t$ th element in  $\mathcal{X}^n \cup \{\perp\}$  (sorted in any fixed order) belongs to  $\mathcal{M}_L(u^{L-1})$ . Define  $\mathbb{D}_{L-1} = \{\mathbf{D}(u^{L-1}) \mid u^{L-1} \text{ over all possible choices for the first } L-1 \text{ flows}\}$ . It is immediate that  $|\mathbb{D}_{L-1}| \leq 2^{|\mathcal{X}|^n + 1}$ . Now if  $\mathbf{D}(u^j)$  and  $\mathbb{D}_j$  is well-defined, we define  $\mathbf{D}(u^{j-1})$  and  $\mathbb{D}_{j-1}$ . Define  $\mathbf{D}(u^{j-1}) = (d_0, d_1, \dots, d_{|\mathbb{D}_j|})$  to be a  $(|\mathbb{D}_j| + 1)$ -dimensional binary vector:  $d_i = 1$  if and only if there exists  $u_j \in \mathcal{M}_j(u^{j-1})$  such that  $\mathbf{D}(u^j)$  is the  $i$ th element in  $\mathbb{D}_j \cup \{\perp\}$ , where  $\mathbb{D}_j \cup \{\perp\}$  is sorted in any fixed order. Similarly, define  $\mathbb{D}_{j-1}$  to be the set of  $\mathbf{D}(u^{j-1})$  over all  $u^{j-1}$ . Continuing the iterative definition till  $\mathbf{D}(u^1)$  and  $\mathbb{D}_1$  is defined. Let  $D_j = |\mathbb{D}_j|$  for each  $j$ . From our definition,  $D_j \leq 2^{1+D_{j+1}}, \forall j$ .

**Claim 2.** If  $\mathbf{D}(u^{j-1}) = \mathbf{D}(\bar{u}^{j-1})$  for some  $u^{j-1}$  and  $\bar{u}^{j-1}$ , then (i)  $\perp \in \mathcal{M}_j(u^{j-1})$  if and only if  $\perp \in \mathcal{M}_j(\bar{u}^{j-1})$ ; (ii)  $u_j \in \mathcal{M}_j(u^{j-1}) \setminus \{\perp\}$  if and only if there exists  $\bar{u}_j \in \mathcal{M}_j(\bar{u}^{j-1}) \setminus \{\perp\}$  such that  $\mathbf{D}(u^j) = \mathbf{D}(\bar{u}^j)$ .

**Proof.** Let  $\mathbf{D}(u^{j-1}) = \mathbf{D}(\bar{u}^{j-1}) = (d_0, d_1, \dots, d_Q)$ . W.L.O.G.,  $\perp$  is the 0th element in  $\mathbb{D}_j \cup \{\perp\}$ . Then, the claim follows from the definition: (i)  $d_0 = 1$  iff  $\perp \in \mathcal{M}_j(u^{j-1})$  and  $\perp \in \mathcal{M}_j(\bar{u}^{j-1})$ ; (ii)  $d_i = 1$  for  $i > 0$  if and only if there exists  $u_j \in \mathcal{M}_j(u^{j-1})$  such that  $\mathbf{D}(u^j)$  is the  $i$ th element in  $\mathbb{D}_j \cup \{\perp\}$ . Especially, under the existence for (ii),  $\mathbf{D}(u^j) = \mathbf{D}(\bar{u}^j)$  is the  $i$ th element in  $\mathbb{D}_j \cup \{\perp\}$ .  $\square$

Now we claim  $|\mathcal{S}| \leq D_1$ ; otherwise, we construct an Oscar who breaks the authentication property as follows. Since  $|\mathcal{S}| > D_1$ , there must exist distinct  $u_1, \bar{u}_1 \in \mathcal{S}$  such that  $\mathbf{D}(u_1) = \mathbf{D}(\bar{u}_1)$ . Then, the code of Oscar is as follows.

- Oscar provides  $u_1$  to Alice as her source state input. When Alice sends  $u_1$  to Bob noiselessly, Oscar revises it to  $\bar{u}_1$  and sends it to Bob.
- Assume the  $(j-1)$ th flow has been handled and  $\mathbf{D}(u^{j-1}) = \mathbf{D}(\bar{u}^{j-1})$ . We handle the  $j$ th flow for  $j < L$  as follows.

- If Alice sends  $u_j$  to Bob ( $u_j \in \mathcal{M}_j(u^{j-1}) \setminus \{\perp\}$ ), then by Claim 2 there exists  $\bar{u}_j \in \mathcal{M}_j(\bar{u}^{j-1}) \setminus \{\perp\}$  such that  $\mathbf{D}(u^j) = \mathbf{D}(\bar{u}^j)$ . Oscar revises  $u_j$  to  $\bar{u}_j$  and sends it to Bob.
- If Alice rejects with a local output  $u_j = \perp$ , then  $\perp \in \mathcal{M}_j(u^{j-1})$  by definition. By Claim 2,  $\perp \in \mathcal{M}_j(\bar{u}^{j-1})$ , Oscar rejects Bob with a local output  $\bar{u}_j = \perp$ .
- The case that Bob sends  $\bar{u}_j$  is handled similarly.
- Finally, when Alice outputs  $u_L = \perp$ , the case is similar to  $u_j = \perp$  for  $j < L$ ; when Alice sends  $u_L \in \mathcal{M}_L(u^{L-1}) \setminus \{\perp\}$  to Bob, Oscar can not change it (in this case, we define  $\bar{u}_L = u_L$ ). However, based on the definition of  $\mathcal{M}_L(u^{L-1})$  and the previous item that  $\mathbf{D}(u^{L-1}) = \mathbf{D}(\bar{u}^{L-1})$ , we know that  $\bar{u}_L \in \mathcal{M}_L(u^{L-1}) = \mathcal{M}_L(\bar{u}^{L-1})$ . When Bob receives  $\bar{u}_L$ , if he outputs  $\bar{u}_1$ , then Oscar succeeds; otherwise, he fails.

Now we analyze the success probability  $p$  of Oscar. First of all, Alice is a sender with a uniformly random tape and especially is admissible. Thus,  $u_j \in \mathcal{M}_j(u^{j-1})$  for any  $j$ . By our analysis in the attack,  $\bar{u}_j \in \mathcal{M}_j(\bar{u}^{j-1})$  as well. Thus, by the definition of *admissible* and the definition of  $\mathcal{M}_L(\cdot)$ , Alice' is an admissible sender in the execution (Alice', Bob). By correctness, Bob will output  $\bar{u}_1$  with probability at least  $1 - \eta > \epsilon$ , contradiction to the authentication property (as  $\bar{u}_1 \neq u_1$ ). Thus,  $|\mathcal{S}| \leq D_1$ . Finally, as  $\log D_j \leq 1 + D_{j+1}$  for any  $j$  (let  $D_L = |\mathcal{X}^n|$ ), Claim 1 implies that  $\log^{(L)} D_1 \leq 1 + \log D_L = 1 + n \log |\mathcal{X}|$ . Hence,  $\log^{(L)} |\mathcal{S}| \leq 1 + n \log |\mathcal{X}|$ . Thus,  $\log^* |\mathcal{S}| = L + \log^*(\log^{(L)} |\mathcal{S}|) \leq L + \log^*(1 + n \log |\mathcal{X}|)$ . This concludes the theorem for  $\pi$  satisfying the restrictions at the beginning.

For the general case, notice that for any  $L$ -round  $\epsilon$  authentication protocol  $\pi$ , by Lemma 8 and Lemma 9, there exists an  $(L+4)$ -round  $(\epsilon + 2^{-\beta n'})$ -secure authentication protocol  $\pi'$  with  $n' = \gamma n$  for some constants  $\beta > 0, \gamma > 0$  that satisfies the restriction at the beginning, where  $n$  and  $n'$  are respectively the number of channel  $W_1$  uses in  $\pi$  and  $\pi'$ . Applying the above proof to  $\pi'$ , we conclude that  $\log^* |\mathcal{S}| \leq L + 4 + \log^*(1 + n\gamma \log |\mathcal{X}|) \leq L + 4 + \log^*(2^n)$  when  $n$  large enough. Hence, the theorem follows.  $\blacksquare$

## VI. LOWER BOUND ON THE SUCCESS PROBABILITY

In this paper, we regard the DMC  $W_1$  as an important resource and hope to minimize the use of it. For a fixed total length of messages over it and a fixed authentication error  $\epsilon$ , we might wish to authenticate a source space as large as possible. However, the following theorem shows that  $\epsilon$  is very dependent on the message space on DMC  $W_1$ .

Our idea is to present an Oscar that achieves a certain success probability. Roughly, when Alice is authenticating  $S$  to Bob, Oscar blocks the communication between Alice and Bob. In addition, Oscar plays the role of 'Bob' to interact with Alice. At the same time, Oscar starts an independent session to play the role of 'Alice' to authenticate a new message  $S'$  to Bob, except that he uses Alice's DMC messages in the previous session as his own. Here two authentication sessions are independent, except that they use the same DMC



messages. By calculation, we can show that two independent sessions share the same DMC messages with probability at least  $2^{-H(F)}$ . When this event occurs, Bob will accept  $S'$ , except a completeness error. So Oscar succeeds with probability at least  $2^{-H(F)} - \delta - \frac{1}{|S|}$ , where  $\frac{1}{|S|}$  accounts for the possibility of  $S = S'$ . The formal detail is as follows.

**Theorem 3:** Let  $\pi$  be an  $\epsilon$ -secure authentication protocol in our model for source space  $S$  with correctness error  $\delta$ . Assume  $F$  is the concatenation of messages over DMC  $W_1$  by Alice (if some flow does not contain a DMC message, use an empty symbol to represent the DMC message in this flow). Let  $\mathcal{F}$  be the space of  $F$ . Then,  $\epsilon \geq 2^{-H(F)} - \delta - \frac{1}{|S|}$ . Especially,  $\epsilon \geq \frac{1}{|\mathcal{F}|} - \delta - \frac{1}{|S|}$ .

**Proof.** We now present a strategy for Oscar to achieve the claimed lower bound. Oscar first generates  $S' \leftarrow S$  and then simulates two parties: Alice' and Bob' to conduct a type I attack (denoted by  $\Gamma$ ) as follows.

- When Alice interacts with Bob for authenticating  $S \leftarrow S$ , Bob' intercepts and blocks all the messages from Alice, except the messages over DMC  $W_1$ . In addition, Bob', in the role of Bob, interacts with Alice faithfully, except that he simulates the output of  $W_1$  using the input from Alice (recall that Oscar can see the input of Alice over  $W_1$ ). In addition, Alice' intercepts and blocks all the messages from Bob. She then interacts with Bob faithfully to authenticate  $S'$ , except that she regards each message over DMC  $W_1$  from Alice as her own message to Bob.

In this attack, Oscar succeeds if and only if Bob outputs  $S'$  (denoted by event **Good**) and  $S' \neq S$ . So  $P(\text{succ}(\text{Oscar})) \geq P(\text{Good}) - P(S' = S) = P(\text{Good}) - 1/|S|$ .

In the following, we analyze  $P(\text{Good})$ . Toward this, we consider a mental variant (denoted by  $\Gamma'$ ) of Oscar's attack  $\Gamma$ , where the difference is as follows.

- Bob' does not use the simulated output of  $W_1$  and instead he can also intercept and block the channel  $W_1$  and use the channel output.
- Alice' does not use the messages  $W_1$  from Alice as her own  $W_1$  messages to Bob. Instead, she can send messages directly onto  $W_1$  and Bob can receive the corresponding output.

In other words, Bob' and Alice' is changed such that (Alice, Bob') and (Alice', Bob) maintain two independent protocol executions, where the former is to authenticate  $S \leftarrow S$  while the latter is to authenticate  $S' \leftarrow S$ .

Let  $F_1$  be the messages over  $W_1$  in execution (Alice, Bob') and  $F_2$  be the messages over  $W_1$  in execution (Alice', Bob). Observe that a simulated  $W_1$  and a real  $W_1$  have the same statistical characteristics. It follows that, conditional on  $F_1 = F_2$ ,  $\Gamma'$  and  $\Gamma$  are distributed identically. Let  $P^\Gamma(\mathbf{E})$  denote the event  $\mathbf{E}$  in an experiment  $\Gamma$ . Then,

$$\begin{aligned} P^\Gamma(\text{Good}) &\geq P^\Gamma(\text{Good}|F_1 = F_2)P^\Gamma(F_1 = F_2) \\ &= P^{\Gamma'}(\text{Good}|F_1 = F_2)P^\Gamma(F_1 = F_2) \\ &\geq P^{\Gamma'}(\text{Good}|F_1 = F_2)P^{\Gamma'}(F_1 = F_2) \\ &\quad (P^\Gamma(F_1 = F_2) = 1 \text{ by definition of } \Gamma) \\ &= P^{\Gamma'}(\text{Good}, F_1 = F_2) \end{aligned} \quad (6)$$

Further, in  $\Gamma'$ , executions (Alice, Bob') and (Alice', Bob) are independent. Also,  $F_1$  is an event in the execution of (Alice, Bob') while  $(\text{Good}, F_2)$  is an event in the execution of (Alice', Bob). So  $F_1$  is independent of  $(\text{Good}, F_2)$ . Thus,

$$\begin{aligned} &\text{Eq. (6)} \\ &= \sum_{a \in \mathcal{F}} P^{\Gamma'}(\text{Good}, F_2 = a) P^{\Gamma'}(F_1 = a) \\ &\geq \sum_{a \in \mathcal{F}} P^{\Gamma'}(F_2 = a) P^{\Gamma'}(F_1 = a) - \delta \\ &\quad /* \text{ execution (Alice', Bob) is faithfully according to } \pi \\ &\quad \text{and so } P^{\Gamma'}(\text{Good}) \geq 1 - \delta. */ \\ &= \sum_{a \in \mathcal{F}} P_F^2(a) - \delta, \\ &\quad /* F_1, F_2 \text{ are i.i.d. according to the corresponding RV } F \\ &\quad \text{of a faithful execution of } \pi. */ \\ &\geq 2^{-H(F)} - \delta, \\ &\quad /* \log(\sum_x P_X^2(x)) \geq -H(X) \text{ as } \log(x) \text{ is concave } */ \end{aligned}$$

This gives the first conclusion. The second one follows from  $H(F) \leq |\mathcal{F}|$ . This completes the proof. ■

## VII. THE CAPACITY OF NON-INTERACTIVE AUTHENTICATION OVER ANY DMC

In this section, we study a non-interactive case of the keyless authentication in our model: the protocol consists only of one message flow  $(X^n, u)$  sent from Alice to Bob, where  $X^n$  is over channel  $W_1$  and  $u$  is over the noiseless channel. The authentication capacity in this setting with BSCs  $W_1$  and  $W_2$  was obtained in [17]. In the following, we extend it to the general DMC setting.

Our idea is as follows. By Lemma 4, we have a subset  $\mathcal{C}$  of size  $|\mathcal{X}^{n(1-\delta)}|$  for an arbitrarily small  $\delta > 0$  such that any two elements in  $\mathcal{C}$  has a large distance. By Lemma 3, if we send  $C_i \in \mathcal{C}$  over DMC, Bob will not confuse it with  $C_j \in \mathcal{C}$ , in the sense of the presence of a type I attack. So  $\mathcal{C}$  can be used to authenticate a source space of size  $|\mathcal{X}|^{n(1-\delta)}$  against type I attack. A type II attack can be combated using the same idea in SetAuth\*. This gives a scheme with an authentication rate of  $(1 - \delta) \log |\mathcal{X}|$ . Since  $\delta$  is arbitrarily small, any rate less than  $\log |\mathcal{X}|$  can be achieved. On the other hand, it is obvious that the rate can not surpass  $\log |\mathcal{X}|$  as the noiseless channel is insecure and hence one codeword over DMC  $W_1$  can authenticate at most one source state.

**Theorem 4:** The capacity of a non-interactive authentication in our model with  $W_1$  non-redundant and  $\text{Cov}(W_1) \not\subseteq \text{Cov}(W_2)$  is  $\log |\mathcal{X}|$ .

**Proof. Achievability.** For any  $\alpha \in (1/n, 1/2]$ , by Lemma 4, there exists  $\mathcal{C} \subseteq \mathcal{X}^n$  such that any two elements in it have distance at least  $\alpha n$  and that  $|\mathcal{C}| \geq \frac{|\mathcal{X}|^{n(1-\alpha-\frac{h(\alpha)}{\log |\mathcal{X}|})}}{\alpha n}$ . Now let  $\mathcal{C} = \{C_1, \dots, C_N\}$ .

Let  $k = \sqrt{n}$ . Since  $\text{Cov}(W_1) \not\subseteq \text{Cov}(W_2)$ , there exists  $a \in \mathcal{X}$  such that  $W_1(\cdot|a) \notin \text{Cov}(W_2)$ . So  $\Delta(W_1(\cdot|a), \text{Cov}(W_2)) = \xi$  for some  $\xi > 0$ . Let  $\epsilon = \min\{\frac{\xi}{4|\mathcal{Z}|}, \frac{\alpha\Theta}{2}\}$  and  $\epsilon' = 2e^{-\frac{k\xi^2}{8|\mathcal{Z}|^2}}$ , where  $\Theta$  is defined in Lemma 3 for the non-redundant DMC  $W_1$ . We construct the protocol for Alice to authenticate  $s \in [N]$  as follows.

1. Alice sends  $a^k|C_s$  over channel  $W_1$  and  $s$  over the noiseless channel.
2. Upon  $Z^{n+k}$  from channel  $W_1$  and  $s'$  from the noiseless channel, Bob checks if  $Z^k \in \mathcal{T}_{[W_1]_\epsilon}^k(a^k)$  and  $Z_{k+1}^{k+n} \in \mathcal{T}_{[W_1]_\epsilon}^n(C_{s'})$ . If yes, he outputs  $s'$ ; otherwise, he rejects.

Consider a type II attack first. Assume Oscar sends  $X^{k+n}$  over  $W_2$ . We claim that  $P_{Z^k}(\mathcal{T}_{[W_1]_\epsilon}^k(a^k)) \leq \epsilon'$  (in other words,  $P_{Z^k}(|T_{Z^k}(u) - W_1(u|a)| \leq \frac{\epsilon}{|\mathcal{Z}|}, \text{ for all } u \in \mathcal{Z}) \leq \epsilon'$ ). Otherwise, by Lemma 2,

$$\begin{aligned} \Delta(W_1(\cdot|a), \text{Cov}(W_2)) &\leq |\mathcal{Z}|\epsilon + |\mathcal{Z}|\sqrt{\frac{\ln(2/\epsilon')}{2k}} \\ &\leq \frac{\xi}{4} + \frac{\xi}{4} < \xi, \end{aligned}$$

which contradicts  $\Delta(W_1(\cdot|a), \text{Cov}(W_2)) = \xi$ . Thus, a type II attack succeeds with probability at most  $\epsilon' = 2e^{-\frac{k\xi^2}{8|\mathcal{Z}|^2}}$ .

We now consider a type I attack. In this case, Oscar succeeds only if  $Z_{k+1}^{k+n} \in \mathcal{T}_{[W_1]_\epsilon}^n(C_{s'})$  for  $s' \neq s$ . However,  $d_H(C_s, C_{s'}) > \alpha n$ . By Lemma 3,

$$W_1(\mathcal{T}_{[W_1]_\epsilon}^n(C_{s'})|C_s) \leq 2^{-\frac{2n(\alpha\Theta - \epsilon)^2}{|\mathcal{X}|^2|\mathcal{Z}|^2}} \leq 2^{-\frac{n\alpha^2\Theta^2}{2|\mathcal{X}|^2|\mathcal{Z}|^2}}, \quad (7)$$

exponentially small!

Authentication rate is  $\lim_{n \rightarrow \infty} \frac{1}{n+k} \log \frac{|\mathcal{X}|^{n(1-\alpha-\frac{h(\alpha)}{\log|\mathcal{X}|})}}{\alpha n} = [1 - \alpha - \frac{h(\alpha)}{\log|\mathcal{X}|}] \log|\mathcal{X}|$ . Since  $\alpha$  is arbitrarily small, any rate less than  $\log|\mathcal{X}|$  can be achieved.

*Converse.* Since any point in  $\mathcal{X}^n$  can be a codeword for at most one source  $s$  (recall the noiseless channel can be modified arbitrarily), the authentication rate is at most  $\log|\mathcal{X}|$ . ■

## VIII. CONCLUSION

In this paper, we further studied the keyless authentication problem in the noisy model of our previous work [17]. We extended the construction in [17]. If the message space is  $\mathcal{S}$  and the number of channel  $W_1$  uses is  $n$ , then our new protocol has a round complexity  $\log^*|\mathcal{S}| - \log^*n + 4$ . Here  $n$  can be chosen independent of  $\mathcal{S}$  while this is impossible in the protocol of [17]. We proved a lower bound  $\log^*|\mathcal{S}| - \log^*n - 5$  on the round complexity. We also obtained a lower bound on the success probability. Finally, we showed the capacity for a non-interactive authentication under general DMCs  $W_1, W_2$  is  $\log|\mathcal{X}|$ , which extends the result under BSCs in [17].

## REFERENCES

- [1] R. Ahlswede, I. Csiszár, “Common randomness in information theory and cryptography. Part I: secret sharing”, *IEEE Transactions on Information Theory*, vol. 39, pp. 1121-1132, 1993.
- [2] H. Ahmadi, R. Safavi-Naini, “Secret Keys from Channel Noise”, in *Proc. Advances in Cryptology-EUROCRYPT 2011*, K. G. Paterson (Ed.), LNCS 6632, pp. 266-283, 2011.
- [3] P. Baracca, N. Laurenti, and S. Tomasin, “Physical Layer Authentication over MIMO Fading Wiretap Channels”, *IEEE Transactions on Wireless Communications*, vol. 11, no. 7, pp. 2564-2573, July 2012.
- [4] J. Barros, H. Imai, A. Nascimento, S. Skludarek, “Bit commitment over Gaussian channels”, in *Proc. IEEE International Symposium on Information Theory 2006*, pp. 1437-1441, 2006.
- [5] M. Bellare, R. Canetti, and H. Krawczyk, a modular approach to the design and analysis of authentication and key exchange protocols, *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing*, pp. 419-428, 1998, Dallas, Texas, USA.
- [6] M. Bellare, S. Tessaro, and A. Vardy, “Semantic security for the wiretap channel”, in *Advances in Cryptology (Lecture Notes in Computer Science)*, vol. 7417, R. Safavi-Naini and R. Canetti, Eds. Berlin, Germany: Springer-Verlag, 2012, pp. 294-311.
- [7] M. Bloch, J. Barros, *Physical Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.
- [8] M. Bloch, J. Barros, S. McLaughlin, “Practical information-theoretic commitment”, in *Proc. Allerton Conference Communication, Control, and Computing 2007*, pp. 1035-1039, 2007.
- [9] C. Crépeau and J. Kilian, “Achieving oblivious transfer using weakened security assumptions”, in *Proc. 29th Annual Symposium on Foundations of Computer Science (FOCS'88)*, pp. 42-52, 1988.
- [10] C. Crépeau, “Efficient Cryptographic Protocols Based on Noisy Channels”, in *Proc. Advances in Cryptology-EUROCRYPT 1997*, J. Borst et al. (Eds.), LNCS 1233, pp. 306-317, 1997.
- [11] C. Crépeau, K. Morozov, S. Wolf, “Efficient unconditional oblivious transfer from almost any noisy channel”, in *Proc. Security in Communication Networks 2004*, C. Crépeau (Ed.), LNCS 3352, pp. 47-59, 2004.
- [12] I. Csiszár and J. Körner, Broadcast channels with confidential messages, *IEEE Transactions on Information Theory*, Vol. IT-24, No. 3, May 1978, pages 339-348.
- [13] I. Csiszár and J. Körner, *Information Theory: Coding Theorem for Discrete Memoryless System*, Cambridge University Press, 2011.
- [14] I. Csiszár and P. Narayan, “Common randomness and secret key generation with a helper”, *IEEE Transactions on Information Theory*, vol. 46, pp. 344-366, 2000.
- [15] E. N. Gilbert, F. J. MacWilliams and N. J. Sloane, “Codes which detect deception”, *Bell System Technical Journal*, Vol 53, No. 3, pp. 405-424, 1974.
- [16] D. R. Hughes and F. C. Piper, *Design Theory*, Cambridge University Press, 1985.
- [17] S. Jiang, Keyless Authentication in a Noisy Model, *IEEE Transactions on Information Forensics and Security*, Vol. 9, No. 6, pp. 1024-1033, 2014.
- [18] S. Jiang, (Im)possibility of Deterministic Commitment over a Discrete Memoryless Channel, *IEEE Transactions on Information Forensics and Security*, Vol. 9, No. 9, pp. 1406-1415, 2014.
- [19] A. Khisti, S. Diggavi, G. Wornell, “Secret key generation with correlated sources and noisy channels”, in *Proc. IEEE International Symposium on Information Theory 2008*, pp. 1005-1009 (2008).
- [20] V. Korzhik, V. Yakovlev, G. M. Luna, R. Chesnokov, “Performance Evaluation of Keyless Authentication Based on Noisy Channel”, In *Proc. MMM-ACNS 2007*, V. Gorodetsky et al. (Eds.), Springer-Verlag, Berlin, pp. 115-126, 2007.
- [21] L. Lai, H. ElGamal and H. V. Poor, “Authentication over noisy channels”, *IEEE Trans. on Inf. Theory*, vol. 55, no. 2, pp. 906-916, Feb. 2009.
- [22] Y. Liang, H. V. Poor, S. Shamai, “Information Theoretic Security”, *Foundations and Trends in Communications and Information Theory*, vol 5, nos 4-5, pp 355-580, Now Publishers, Hanover, MA, USA, 2008.
- [23] U. Maurer, “Secret key agreement by public discussion from common information”, *IEEE Transaction on Information Theory*, vol. 39, pp. 733-742, 1993.
- [24] U. Maurer and S. Wolf, “Secret-key agreement over unauthenticated public channels - part I: definitions and a completeness”, *IEEE Transactions on Information Theory*, vol. 49, pp. 822-831 (2003).
- [25] E. Martinian, G.W. Wornell, and B. Chen, “Authentication with distortion criteria”, *IEEE Transactions on Information Theory*, vol. 51, pp. 2523-2542, 2005.
- [26] A. Nascimento and A. Winter, “On the oblivious transfer capacity of noisy correlations”, in *Proc. IEEE International Symposium on Information Theory 2006*, pp. 1871-1875, 2006.
- [27] R. Rivest, A. Shamir and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems”, *Communications of ACM*, vol. 2, pp. 120-126, February 1978.
- [28] P. L. Yu, J. S. Baras, and B. M. Sadler, Physical-layer authentication, *IEEE Trans. Inf. Forensics and Security*, vol. 3, no. 1, pp. 38-51, Mar. 2008.
- [29] A. Winter, A. Nascimento, and H. Imai, “Commitment capacity of discrete memoryless channels”, in *Proc. 9th IMA Conf. Coding and Cryptography (WCC 2003)*, K.G. Paterson (Ed.), LNCS 2898, pp. 35-51, 2003.
- [30] A. D. Wyner, “The wire-tap channel”, *Bell System Technical Journal*, vol. 54, pp. 1355-1367, 1975.